العنوان:	تجربة دولة الامارات فى التصدى للجرائم المعلوماتية الواقعة على التجارة الالكترونية
المصدر:	المجلة الأردنية للمكتبات والمعلومات - جمعية المكتبات والمعلومات الأردنية - الأردن
المؤلف الرئيسي:	حوتية، عمر
مؤلفين آخرين:	سيد، رحاب فايز أحمد(م. مشارك)
المجلد/العدد:	مج50, ع4
محكمة:	نعم
التاريخ الميلادي:	2015
الشهر:	كانون الأول
الصفحات:	127 - 174
رقم MD:	747770
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	الجرائم المعلوماتية، التجارة الإلكترونية، الإمارات العربية المتحدة
رابط:	http://search.mandumah.com/Record/747770

تجربة دولة الإمارات في التصدي للجرائم المعلوماتية الواقعة على التجارة الالكترونية

أ. عمر حوتية(*)
جامعة أدرار - الجزائر
د. رحاب فايز أحمد سيد(**)
جامعة بني سويف - مصر

المستخلص:

تعتبر التجارة الالكترونية إحدى أهم المظاهر الحديثة في اقتصاد المعرفة والمحرك الأساسي له، وفي ظل ما يشهده العالم من تغيرات كبيرة شملت مختلف القطاعات، سعت دولة الإمارات إلى تعظيم دور التجارة الالكترونية، وكان لذلك أثره في الدفع بعجلة التنمية الاقتصادية وتعزيز التنافسية الوطنية للإمارات، وجعل تجربتها رائدة في بناء أسس اقتصاد المعرفة.

وبالنظر للتطور المتسارع لشبكة الانترنت، والاعتماد شبه الكامل على الفضاء الإلكتروني، زادت معدلات انتشار الجرائم المعلوماتية، وهو ما يستدعي وضع استراتيجيات فعالة للتأمين على مخاطر الجرائم المعلوماتية الناجمة عن استخدام الفضاء الالكتروني في التعاملات التجارية.

(*)hotiamar@yahoo.fr

(**)Dr.rehab.yousef@art.bsu.edu.eg

وسنحاول من خلال هذا البحث الإجابة على الاشكالية التالية:

ما هي خصائص التجربة الإماراتية في التصدي للجرائم المعلوماتية الواقعة على التجارة الالكترونية؟

وتهدف هذه الدراسة إلى إلقاء الضوء على ماهية الجرائم المعلوماتية، ووصف جهود دولة الامارات العربية المتحدة في الحدّ من مخاطر الجرائم المعلوماتية الناجمة عن استخدام الفضاء الالكتروني في التعاملات التجارية. وإبراز أهمية استفادة الدول العربية من التجربة الاماراتية في التصدي لجرائم التجارة الالكترونية، حيث شكل القانون رقم 2/ 2006 بشأن مكافحة جرائم تقنية المعلومات كقانون استرشادي عربي.

الكلمات المفتاحية:

التجارة الإلكترونية، الجريمة المعلوماتية، القرصنة، مكافحة الجريمة الإلكترونية، التجربة الإمارتية.

مقدمة:

يقوم الاقتصاد الرقمي على عدة عناصر أهمها القطاعات المنتجة والمستخدمة لتقنية المعلومات، وقطاعات خدمات الاتصالات، والتجارة الالكترونية، وتعد هذه الأخيرة أحد ثمار الثورة المعلوماتية، ومن المتوقع أن تكون أسلوب التجارة السائد بين المنظمات والأفراد خلال هذا القرن في كافة أنحاء العالم.

وتسعى العديد من الدول ومنها دولة الإمارات العربية المتحدة إلى تعظيم دور التجارة الالكترونية في اقتصادها إلا أنها تواجه العديد من المعوقات والتحديات، ومن أهمها الانتشار الواسع للجرائم الإلكترونية، فزيادة استخدام الإنترنت أو الحاسوب في التعاملات التجارية سيجعله معرضا لهجمات فيروسية أو تجسسية.

1- اشكالية الدراسة:

إن الانتشار الواسع للجرائم المعلوماتية الواقعة على التجارة الالكترونية، يستدعي دراسة تأثيراتها ومن ثم وضع استراتيجية واضحة المعالم للحد من الآثار والمخاطر الناجمة عن هذا النوع من الجرائم المعلوماتية.

فما هي خصائص التجربة الإماراتية في التصدي للجرائم المعلوماتية الواقعة على التجارة الالكترونية؟

2- أهمية الدراسة:

ترجع أهمية موضوع الدراسة لارتباطها بالجريمة المعلوماتية التي أصبحت مُتلازمة مع الطفرة الهائلة في مجال تكنولوجيا الاتصالات والمعلومات، وبالشكل الذي أصبح فيه الأمن المعلوماتي مُهدداً بأساليب إجرامية لم يعرفها القانون من قبل. أضف إلى ذلك ما ترتب على ظاهرة العولمة وثورة الاتصالات والمعلومات من ظهور مفهوم الجريمة العابرة للحدود، والتي أضحت ظاهرة دولية يتعدى خطرها وضررها نطاق الدولة الواحدة، مما يستدعي ايجاد السبل لمواجهتها.

3- أهداف الدراسة:

تهدف الدراسة إلى تحقيق عدة أهداف، نوجزها بشكل خاص فيما يلي:

1) إلقاء الضوء على ماهية الجرائم المعلوماتية، وأنواعها وأسباب انتشارها.

2) الإشارة إلى الجهود التي تبذلها دولة الامارات العربية المتحدة في مُكافحة الجرائم المعلوماتية.

3) ابراز أهمية استفادة الدول العربية من التجربة الاماراتية في التصدي لجرائم التجارة الالكترونية،

4- حدود الدراسة:

4/ 1 الحدود الموضوعية: تتناول الدراسة الجرائم المعلوماتية المتعلقة بالتجارة الالكترونية مع التركيز على تجربة الإمارات.

4/ 2 الحدود النوعية: تقتصر الدراسة على جرائم التجارة الإلكترونية فقط دون التطرق للجرائم المعلوماتية الأخرى.

4/ 3 الحدود اللغوية: تتناول الدراسة النتاج الفكري فيما يتعلق بالجرائم المعلوماتية والتجارة الإلكترونية.

5- منهج الدراسة:

اتبعت الدراسة المنهج الوصفي التحليلي الذي يسعى للتعريف بالجرائم الواقعة على التجارة الالكترونية، وتحليل وتشخيص موضوع الدراسة من مُختلف جوانبها وأبعادها، بهدف التوصل إلى نظرة واضحة عن الآليات المُلائمة لُمكافحة هذه الظاهرة المُستحدثة، بالنظر لنتائج التجربة الإماراتية، كما تم اتباع دراسة الحالة لدراسة التجربة الإماراتية المتعلقة بهذا الشأن.

6- الدراسات السابقة:

1) جاءت دراسة الشيخ والراشد (El-Sheikh, & Al- Rashed, 2004) بهدف دراسة أثر البيئة التعليمية والمناهج الدراسية الموجودة على مستوى المعرفة بمخاطر قرصنة البرمجيات والحد منها. حيث أوصت الدراسة إدارة الجامعات والمنظمات التعليمية بالاهتمام بإقامة الندوات والمحاضرات والمؤتمرات وكذلك تشجيع نشر الأبحاث العلمية والمقالات المحكمة وتوجيه المعلمين والمشرفين التربويين للتركيز على موضوع قرصنة البرمجيات وطرق مكافحتها، كما أوصت

الدراسة بضرورة العمل على تطوير منهاج دراسي متكامل للمساهمة بصورة فعالة في مكافحة هذه الظاهرة.[1]

2) أجرى الضراب (Al-Dharrab, 2005) دراسة عن استخدام طريقة البصمة المائية للحد من قرصنة البرمجيات وحماية حقوق الملكية الفكرية، وتم من خلالها وضع طريقة مبتكرة وضوابط لإختبار وتقييم التقنيات المختلفة لوضع البصمة المائية في البرمجيات وبالتالي إمكانية قياس فعالية وكفاءة تقنيات البصمة المائية في البرمجيات الحالية أو المستقبلية.[2]

3) قام الشيخ وراشد والقضاه وبيس (El-Sheikh, Rashed, Al-Qudah, & Peace, 2006) بدراسة للكشف عن قرصنة البرمجيات في الأردن بغية الوصول الى حلول، فكانت التوجهات أنه في حين تقع مسؤولية توعية الطلبة بحقوق الملكية الفكرية ومخاطر القرصنة على قطاع التعليم فإن توعية عامة الشعب تقع على عاتق الحكومة والقطاع الخاص. والتأكيد بأن زيادة الوعي مفتاح القدرة للحد من ظاهرة القرصنة.[3]

4) أكد هيندوجا (Hinduja, 2008) أن دراسة السلوك الاجتماعي يمكن أن يحد من انتشار القرصنة، وبنى دراسته على فرضية أن الشخص المقرصن ليس لديه ميول

---

(1)El-Sheikh, Asim, Rashed, Abdullah & Peace, A. Gaham (2004), Software Piracy: Possible Causes and Cures.- Available at: http://www.drpeace.com/m493s05/Piracy.doc

(2)Al-Dharrab, Mohannad (2005) Benchmarking Framework For Software Watermarking.- King Fahd University of Petrolume and Minerals.- Available at: http://library.kfupm.edu.sa/Theses/Details.aspx?Shelflist_number=A+1.D435&Comm_Advisor_ID=40

(3)El-Sheikh, A., Rashed, A., Al-Qudah, B. and Peace, A. (2006) An Exploratory Study of Software Piracy in Jordan.- The Electronic Journal on Information Systems in Developing Countries, vol 23.- Available at: https://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/188/146

للمشاركة مع الآخرين أو اهتمام بهم وابتكاراتهم ويميل للوحدة وقضاء معظم الأوقات والمناقشات عبر الانترنت وهو أكثر ميلا لقرصنة البرمجيات.(1)

وتختلف الدراسة الحالية عن الدراسات السابقة في تناولها الجرائم المعلوماتية المتعلقة بالتجارة الالكترونية والتركيز على تجربة دولة الامارات العربية المتحدة في التصدي لمثل هذا النوع من الجرائم.

7- خطة البحث:

تم معالجة موضوع الدراسة من خلال خطة تتضمن المحاور التالية:

أولا: ماهية الجرائم المعلوماتية الواقعة على التجارة الالكترونية.

ثانيا: تطور التجارة الالكترونية بالإمارات وتزايد مخاطر الجرائم المعلوماتية.

ثالثا: استراتيجيه الإمارات في التصدي للجرائم الواقعة على التجارة الالكترونية.

أولا: ماهية الجرائم المعلوماتية الواقعة على التجارة الالكترونية

تمثل الجرائم الإلكترونية تحديا كبيراً لإدارة نظم المعلومات لما تسببه من خسارة كبيرة للأشخاص وللمنظمات وللدول بشكل عام، فما هي الجريمة المعلوماتية، وما علاقتها بالتجارة الالكترونية.

1- مفهوم التجارة الالكترونية:

ساهم انتشار تكنولوجيا المعلومات في تطور مختلف مجالات الحياة، ومنها التجارة التقليدية وتحولها إلى تجارة الكترونية (E-Commerce)(*). فما مفهوم التجارة الالكترونية؟.

---

(1)Hinduja, Sameer. (2008) Deindividuation and Internet Software Piracy. Cyberpsychology & Behavior, Vol.11 (4).- Available at: http://online.liebertpub.com/doi/abs/10.1089/cpb.2007.0048

1-1- تعريف التجارة الالكترونية:

كثيرة هي التعريفات التي وردت في التجارة الإلكترونية من المشرع أو الفقه، فقد عرفها المشرع التونسي من خلال قانون المبادلات والتجارة الإلكترونية وتحديدا في المادة الثانية منه بأنها:

"العمليات التجارية التي تتم عبر المبادلات الإلكترونية"(1). وفي إمارة دبي نجد أن المشرّع الإماراتي عرّفها بأنها: "المعاملات التجارية التي تباشر بواسطة المراسلات الإلكترونية"(2).

وفي فرنسا تم تعريف التجارة الالكترونية بأنها: "مجموعة من المعاملات الرقمية المرتبطة بأنشطة تجارية بين المشروعات بعضها ببعض وبين المشروعات والأفراد وبين المشروعات والإدارة"(3).

أما منظمة التجارة العالمية فتنظر للتجارة الالكترونية بأنها: "مجموعة متكاملة من =

(*) التجارة الإلكترونية ظاهرة حديثة عرفت منذ بداية التسعينيات للقرن الماضي، وكان أول استخدام لهذا المفهوم سنة 1997 في شركة I.B.M لتمييز أنشطة الأعمال الالكترونية عن أنشطة التجارة الالكترونية. وتصنف عالمياً ضمن نطاق الخدمات وأدرجت في تقرير منظمة التجارة العالمية (WTO) للخدمات في 17/ 3/ 1999.

أنظر: لونيس نادية، أثر تكنولوجيا المعلومات والاتصالات في تفعيل الأعمال التجارية للمؤسسات، رسالة ماجستير، جامعة الجزائر 3، 2011، ص82.

(1) صدر هذا القانون في 9/ 8/ 2000م منشور في الرائد الرسمي للجمهورية التونسية 11/ 8/ 2000م.

(2) المادة الثانية من قانون المعاملات والتجارة الإلكترونية رقم 02/ 2002 بإمارة دبي، تاريخ النشر: 2002-02-16.

(3) عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية العربية، جزء1، دار الفكر الجامعي، الإسكندرية، 2002، ص18.

عمليات عقد الصفقات وتأسيس الروابط التجارية وتوزيع وتسويق وبيع المنتجات عبر شبكة الانترنيت".

ويطلق" رأفت رضوان "مفهوم التجارة الالكترونية على مجمل الخدمات التجارية التي تعتمد على الوسائل الالكترونية كالتبادل الالكتروني للبيانات والتحويلات الالكترونية للأموال والبريد الالكتروني والنشرات الالكترونية وغيرها من الخدمات التي تتعامل بها المؤسسات والشركات"[1].

ويمكن أن نستخلص التعريف التالي: التجارة الالكترونية هي تنفيذ كل ما يتصل بعمليات شراء وبيع البضائع والخدمات والمعلومات بين متعاملين اقتصاديين عن طريق تقنية الاتصال الحديثة المتمثلة في الانترنت، بما يتضمن فعالية وسرعة الأداء.

ولقد أباح الدين الإسلامي، بل رغب وحض على التجارة بكافة أنواعها، وكون التجارة الإلكترونية هي تطوير للتجارة التقليدية العادية، فهي تطوير في وسيلة العمل التجاري في مجال تكنولوجيا المعلومات والاتصالات لا في حقيقته، لذلك وفي الفقه الإسلامي فإنها تقع في دائرة المباح التي تتسع لكل جديد ما دام يحقق مقصدا مشروعا من مقاصد الشريعة الإسلامية [**]، ولا شك أن تطوير التجارة وتحديثها وتيسير التعامل بين الناس يعد من المنافع المباحة.

(1) رأفت رضوان، عالم التجارة الالكترونية، بحوث ودراسات، المنظمة العربية للتنمية الإدارية، 1999، ص348.

(**) أفتى مجلس مجمع الفقه الإسلامي المنعقد بجدة من 14- 20 مارس 1990م، بجواز إبرام عقود التجارة الإلكترونية وشرعية ذلك، وتكييفه في الفقه الإسلامي تظهر في الشروط المعتبرة في العقود التجارية وهي: الرضائية، والثبوتية العقدية، وإمكانية الالتزام تسلماً وتسليماً، مما يحقق حرية التعاقد.

2-1- أهمية التجارة الإلكترونية ومكونات البنية التحتية لها:

يشهد النظام الإلكتروني في المعاملات التجارية انتشارا دوليا فائق السرعة، على حساب النظام الورقي والتقليدي (مثّل أكثر من60٪ من التعاملات التجارية خلال العقدين الأخيرين) نظرا لمزاياه ولا سيما السرعة الخيالية لإنجاز التعاقدات والمدفوعات، والتوفير الكبير في تكاليف التعاملات.

وقد ترك تنامي حجم التجارة الالكترونية عالميا أثره الاقتصادي على ثلاثة مستويات:

1- على مستوى قطاع الأعمال، حيث تتلخص أبرز فوائد التجارة الإلكترونية على مستوى المؤسسات والشركات التجارية في: توسيع نطاق السوق، تفعيل مفهوم المنافسة الكاملة في السوق، انخفاض تكاليف العمليات التجارية، تحكم أفضل في إدارة المخزون.

2- على مستوى المستهلكين، حيث تتحقق الفوائد التالية للمستهلك الالكتروني: سرعة وسهولة التسّوق، تعدد الخيارات، انخفاض الأسعار، سرعة وسهولة تبادل المعلومات بين المستهلكين.

3- على المستوى القومي، أين تساهم في دعم: التجارة الخارجية، التنمية الاقتصادية، التوظيف...الخ.

ونظرا لأهمية التجارة الالكترونية فإنه يتطلب توفر بنية تحتية الكترونية للقيام بتعاملاتها، وتشمل[1]:

---

(1) ثناء أبا زيد، "واقع التجارة الإلكترونية والتحديات التي تواجهها عربياً ومحلياً"، مجلة جامعة تشرين للدراسات والبحوث العلمية، سلسلة العلوم الاقتصادية والقانونية، المجلد (27) العدد (4) 2005.

الأجهزة، البرمجيات، مقدمو خدمات التوصيل بالشبكات العامة المفتوحة، والخدمات المخولة.

وبالإضافة إلى البنية الإلكترونية لابد من توفر البيئة المالية المناسبة لوسائل وأنظمة الدفع والسداد الملائمة لمتطلبات هذه التجارة، وتشمل: بطاقات الاعتماد الإلكترونية Credit Cards، الأساليب البنكية الحديثة في الدفع والسداد، النقود الإلكترونية الرقمية والصكوك (الشيكات الإلكترونية).

2- مفهوم الجرائم المعلوماتية:

إن الاعتماد المتزايد على تكنولوجيا المعلومات جعلها هدفاً جذاباً لارتكاب مختلف الجرائم المعلوماتية[*]، والتي تعد من أعقد وأكثر الجرائم في وقتنا الراهن، فما مفهوم الجرائم المعلوماتية؟.

2-1- تعريف الجريمة المعلوماتية:

رغم اتفاق الفقه على سمات العالم الالكتروني، وصفات المجرم المعلوماتي، إلا أن الآراء تعددت بشأن تعريف الجريمة المعلوماتية، وانقسم الفقه إلى أربعة اتجاهات تقوم على أسس مختلفة، وهي[1]:

(*) هناك مصطلحات مختلفة للجريمة المعلوماتية، منها جريمة الحاسوب computer crime ثم الجريمة السيبرية cyber crime والجريمة الإلكترونية e-crime (على غرار التجارة الإلكترونية e-commerce) والجريمة الرقمية...الخ. وتشير هذه المصطلحات عموما إلى نشاط إجرامي يكون فيه الحاسوب أو الشبكة أداة أو هدفاً أو مكاناً لارتكاب الجريمة المعلوماتية. أنظر: رحاب فايز أحمد سيد، جرائم الكتب الإلكترونية: دراسة تحليلية لوضع استراتيجية حماية لها، مجلة أعلم (قيد النشر)، الاتحاد العربي للمكتبات والمعلومات، 2014.

(1) غازي عبد الرحمان هيان الرشيد، "الحماية القانونية من جرائم المعلوماتية (الحاسب والانترنت)"، أطروحة لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004، ص106.

1- على أساس وسيلة ارتكاب الجريمة، فطالما أن وسيلة ارتكاب الجريمة هو الحاسوب أو إحدى وسائل التقنية الحديثة المرتبطة به فتعتبر من جرائم الانترنت[1]، ويصفها الفقيه الألماني تاديمان بأنها: "كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي"[2]. كما تعرف بأنها « أي فعل ضار يقوم به الفرد عبر استعماله الوسائط الإلكترونية مثل الحواسيب، وأجهزة الموبايل، وشبكات الاتصالات الهاتفية، وشبكات نقل المعلومات، وشبكة الإنترنت، أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية"[3].

2- على أساس توافر المعرفة بتقنية المعلومات، حيث تعرف وزارة العدل الأمريكية هذه الجرائم بأنها:" أية جريمة لفاعلها معرفة فنية بتقنية الحاسبات يمكنه من ارتكابها"[4]. ويعرفها الفقيه الفرنسي Masse بأنها:

"الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح"[5].

3- على أساس موضوع الجريمة، حيث ترى منظمة الأمم المتحدة بأنها: "كل تصرف غير مشروع من أجل القيام بعمليات إلكترونية تمس بأمن الأنظمة المعلوماتية والمواضيع التي تعالجها." [6]

---

(1)Kurbalua Jovan , Gelbestein Eduardo ,Gouvernance de l'internet – enjeux , acteurs et factures , publie par diplofoundation et global knowledge partnership , Suisse , 2005 , p.98.

(2) عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، 2006، ص24.

(3)David Icove, Karl Seger & William Von Storch, Computer Crime, a Crime Fighter's Handbook, New Jersey: Prentice Hall , August 1995.P4.

(4) محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، دار النهضة العربية، القاهرة، 2005، ص34.

(5) محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مطابع الهيئة المصرية العامة للكتاب، 2003، ص19.

(6) Mohamed ChaIwki ,Essai sur la notion de cybercriminalité, juillet 2006, p.7. site: www.iehei.org.

4- اتجاه يأخذ بدمج عدة تعاريف، بعد فشل الاتجاهات السابقة في وضع تعريف شامل للجريمة الالكترونية يتضمن كافة أرجائها، حيث تعرف بأنها: "الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك، أو جريمة يكون الحاسب نفسه ضحيتها".

وبناء على ما سبق يمكن الاستناد إلى التعريف التالي للجرائم المعلوماتية:

الجريمة المعلوماتية: هي نشاط إجرامي يتضمن اعتداءاً على الأفراد أو الممتلكات يرتكب باستخدام المنظومات المعلوماتية من تجهيزات وشبكات حاسوبية، أو تقع على هذه المنظومات، ويترتب عليه وصول غير مشروع إلى معلومات أو موارد تم تخزينها، بهدف النسخ أو الإلغاء أو النقل أو التخريب أو التجسس أو العبث بها.

ويمكن التمييز بين الجريمة المعلوماتية والجريمة التقليدية، مثلما يبنه الجدول التالي:

الجدول رقم (1): بعض الفروقات بين الجريمة التقليدية والجريمة المعلوماتية

الجريمة التقليدية	الجريمة المعلوماتية
- جريمة اعتداء معروفة على حقوق الآخرين كالسرقة والاحتيال والابتزاز والتجسس والتزوير. - معظم الجرائم التقليدية تتم داخل حدود دولة معينة. - وجود نصوص وتشريعات كافية للتعامل معها، وامتلاك خبرات مستفيضة لاكتشاف مرتكبيها. - لها نظير وسند قانوني،	- اعتداء على الأفراد والممتلكات تكون أداتها شبكة الإنترنت أو نظام الحاسوب. - غالبا ما تتجاوز حدود الدول نظراً للطبيعة الخاصة التي تفرضها شبكة الانترنت. - تعتبر حديثة جداً، لذا لا يتمتع القائمون على تطبيق القانون بخبرة كافية للتعامل معها. وتخلو نصوص القانون من المعالجة الوافية لأنواع كثيرة منها مما يتيح لمرتكبيها الإفلات من العقاب. - هناك جرائم لها نظير تقليدي لكنها مختلفة من حيث إمكانية التعامل معها قضائياً· من ذلك: إرسال بريد إلكتروني منتحلاً اسم وصفة شخص آخر بقصد الإضرار بسمعة

الجريمة التقليدية	الجريمة المعلوماتية
ويمكن للقاضي التعامل معها في ظل مواد القانون المعتادة.	ذلك الشخص. فيمكن التعامل مع هذا الفعل في ظل مواد القانون المعتادة بشأن الاحتيال، لكن المشكلة أن القاضي عندما ينظر في القضية قد يجد أن نصوص القانون التي تشير صراحة إلى الكتابة والتوقيع لا تنطبق على البريد الإلكتروني الذي لا يحتاج إلى الورقة والقلم.

المصدر: من إعداد الباحثين.

فبالمعنى الواسع تعتبر الجرائم المعلوماتية جرائم تقليدية معروفة مثل السرقة والاحتيال والابتزاز والتجسس والاختلاس والتزوير، لكن ما يميزها اختيار الفاعل لشبكة الانترنت لتحقيق هدفه بدقة.

وقد ساهم انتشار العديد من التقنيات المعلوماتية في تسهيل ارتكاب مثل هذه الجرائم، ومنها: القرصنة (Hacking)، البرامج الضارة (Malware)، الهجوم على خادم (DNS)، إرسال رسائل مزعجة على البريد الالكتروني (Spam)، سرقة الهوية (Identity Theft)، الابتزاز(Extortion).

2-2- تصنيف الجرائم المعلوماتية:

لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم المعلوماتية نظرا لتشعبها وسرعة تطورها. وبحسب المنظمة الاجتماعية والاقتصادية لغرب آسيا- الاسكوا - التابعة لمنظمة الأمم المتحدة، يمكن تصنيف الأعمال كجرائم معلوماتية، على النحو التالي[1]:

1) التعدي على البيانات المعلوماتية، بالدخول غير المشروع لها بهدف نسخها،

1 فاديا سليمان، الجرائم المعلوماتية وأثرها على العمليات المالية والمصرفية، مجلة الدراسات المالية و المصرفية- العدد الاول لسنة 2015، الأكاديمية العربية للعلوم المالية والمصرفية، عمان، الأردن، ص ص: 8،9.

تغييرها أو اتلافها،أو اعتراضها أثناء نقلها على الشبكة كعمليات التجسس على خطوط الاتصال والتقاط البيانات.

2) التعدي على الأنظمة المعلوماتية، والولوج غير المشروع إليها، كسرقة كلمات المرور أو اختراق هذه الأنظمة وزرع الملفات والفيروسات بهدف التجسس وسرقة المعلومات أو تخريب هذه الأنظمة.

3) إساءة استعمال الأجهزة أو البرامج المعلوماتية، وتتضمن جرائم تقديم أو نشر أو بيع التجهيزات والبرمجيات للقيام بأحد الجرائم السابقة، كتصميم وبيع أو الترويج للفيروسات أو برمجيات اختراق.

4) الجرائم على الأموال، وتتضمن جرائم سرقة أو اختلاس الأموال باستخدام الوسائل المعلوماتية، وجرائم التسويق أو الترويج غير المرغوب فيه، والجرائم المتعلقة بالترويج غير المشروع لأسعار العملات الوطنية أو أسعار الأسهم للتأثير في أسعار الصرف وسوق الأسهم وفي الاقتصاد الوطني.

5) الاستغلال الجنسي للقاصرين، وتتضمن انتاج أو إرسال أو نشر الصور الإباحية والأفلام أو الرسائل النصية أو أية اشارات توجه للقاصرين بهدف استغلالهم جنسياً.

6) التعدي على الملكية الفكرية للأعمال الرقمية، وهي تتضمن وضع اسم على كتاب إلكتروني أو برمجيات وتطبيقات أو أية أعمال فكرية رقمية وبيعها أو وضعها للتداول دون حق ملكية.

7) جرائم السطو على أرقام البطاقات الائتمانية، والتي تعد نقوداً إلكترونية، والاستيلاء عليها يعد استيلاء على مال الغير[1]. أو اختراق الأنظمة المصرفية

(1) Grabosky, P. Electronic Crime ,New Jersey: Prentice Hall, 2006, p.15.

وسحب أو تحويل الأموال بين الحسابات، أو انشاء نقود إلكترونية وطرحها للتداول دون الحصول على التراخيص اللازمة.

8) الجرائم التي تمس بالمعلومات الشخصية، وتتضمن الجرائم المتعلقة بمعالجة أو نشر أو افشاء المعلومات الشخصية، دون الحصول على تصريح مسبق، حتى لو كانت هذه المعلومات صحيحة.

9) جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية، وتشمل جرائم الترويج لمعلومات عنصرية وضد الإنسانية، أو التهديد والتعدي على الأشخاص لانتمائهم العرقي أو المذهبي أو اللون.

10) جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية، وتشمل تملك مواقع إلكترونية للمقامرة على الإنترنت أو الترويج للمخدرات والكحول للقاصرين على الإنترنت أو باستخدام رسائل نصية.

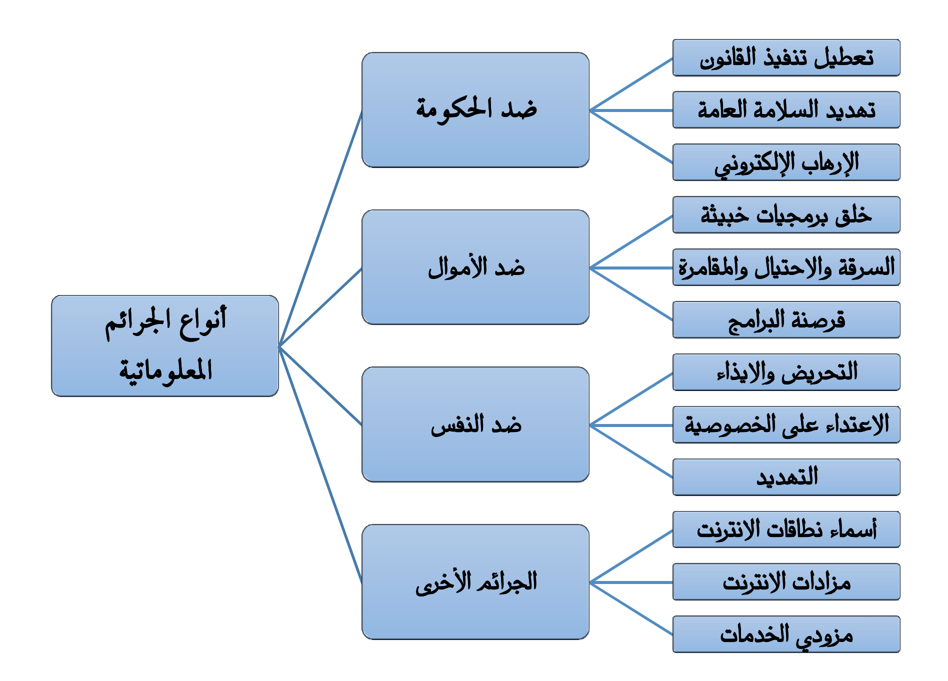
11) جرائم المعلوماتية ضد الدولة والسلامة العامة، وتشمل جرائم النشر أو الترويج لمعلومات الدولة وأمنها واستقرارها أو نظامها القانوني، بما في ذلك جرائم تعطيل أجهزة الدولة ومؤسساتها، أو العبث بالأدلة الجنائية المعلوماتية أو الترويج لأعمال الإرهاب بوسائل معلوماتية.

12) جرائم تشفير المعلومات، وتشمل جرائم توزيع أو نشر أو بيع أو تسويق أو تصدير واستيراد وسائل تشفير دون الحصول على ترخيص من الجهات الرسمية المختصة في الدولة.

وهناك من يصنف الجرائم المعلوماتية حسب الجهة المتضررة منها، مثلما يبينه الشكل التالي:



الشكل رقم (01): تصنيف الجرائم المعلوماتية حسب الجهة المتضررة منها



المصدر: رحاب فايز أحمد سيد، مرجع سبق ذكره.

وهناك العديد من العوامل التي ساعدت على انتشار هذه الجرائم، يمكن حصرها فيما يلي[1]:

1. انفتاح شبكة المعلوماتية: ذكرنا سابقا أن عالم المعلوماتية، فضاء مفتوح على مصراعيه لا يخضع للرقابة والملكية، الأمر الذي سهل عمليات التسلل إليه واختراقه.

---

(1) أخام بن عودة زواوي مليكة، تحديات ظاهرة الجريمة العابرة للأوطان والثورة المعلوماتية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس/ ليبيا، 27-30 اكتوبر 2009، ص10.

2. انعدام الحواجز الجغرافية بين الدول.

3. صعوبة كشف هوية المستخدم: فأي شخص يمكنه انتحال شخصية، أو التخفي بصفة إنسان وهمي

4. بساطة التعامل مع الوسائل التكنولوجية وزهد أثمانها.

5. صعوبة التحقق وإثبات الجرائم.

6. الثغرات القانونية بين مختلف الدول: فما هو صارم في نظام ما مخفف في آخر، مما يتيح الفرصة للمجرمين سرعة التكيف والأنتقال من نقطة جغرافية لآخرى أكثر أمانا.

7. إشكالية الاختصاص القضائي والقوانين الواجب تطبيقها.

فهذه الأسباب تساعد الجماعات الإجرامية على المضي قدما في أنشطتها دون خوف وبكل أمان.

وسوف نركز في هذه الدراسة على جرائم النصب والاحتيال في التجارة الالكترونية.

3- جرائم النصب والاحتيال الواقعة على التجارة الالكترونية:

تُعتبر جريمة النصب والاحتيال التّجاري الالكتروني من أشهر الجرائم المعلوماتية، وقد أصبحت من القضايا الرّئيسيّة في مفاوضات منظّمة التّجارة العالميّة، وتحتاج لجهود واستراتيجيات دولية ومحلية لمواجهتها.

3-1- تعريف جرائم النصب والاحتيال التّجاري الالكتروني:

من الصعوبة إيجاد تعريف محدّد لمفهوم الاحتيال التّجاري الالكتروني، ومن بين تعريفاته:

"يتضمّن الاحتيال استخدام الكذب أو الخداع أو التّضليل للحصول على ميزة

أو مصلحة غير مستحقّة، وكانت من حقّ طرف آخر"[1]. فالاحتيال مثله مثل كافّة الجرائم الأخرى يتضمّن ثلاثة عناصر رئيسيّة، وهي الدّافع من حيث وجود العامل المحرّك للإرادة والذي يُوجّه السّلوك الاحتيالي كالانتقام والبغضاء وغيرها، ووجود الهدف أو الضّحية للسّلوك الاحتيالي، وغياب القدرة على توفير الحماية.

كما يتمثل الاحتيال الالكتروني في أيّ تصرّف أو سلوك متعمّد يحدث من فرد أو العديد من الأفراد يرهق أو يتسبب في أعباء إضافيّة على أيّة أطراف أخرى نتيجة استخدام ممارسات غير أخلاقيّة للحصول على ميزة غير عادلة أو غير قانونية[2]. ويمكن تحديد تعريف للاحتيال التّجاري الالكتروني من خلال التّركيز على الدّوافع، وبشكل يتّسق مع التّطورات المعاصرة، فيُعرّف الاحتيال التّجاري في البيئة الالكترونيّة بأنّه: "هو كل فعل أو ممارسة غير أخلاقيّة تُستخدَم فيها تقنيّات المجتمع الالكتروني وتهدف إلى تحقيق كسب مادّي غير مشروع."[3]

باختصار تعني جرائم الاحتيال التّجاري الالكتروني: "الاستيلاء على أموال الغير بوسيلة يشوبها الخداع"، وتقوم على ثلاثة أركان: الركن المادي وهو وسيلة الاحتيال، محل الجريمة أو موضوعها، والقصد الجنائي.

---

(1) Internet Fraud Complaint Center (IFCC) (2001), Six-Month Data Trends Report, Prepared by the National White Collar Crime Center and the Federal Bureau of Investigation, May-November, 2000.

(2)Internet Fraud Complaint Center (2005), IC3 2004 Internet Fraud: Crime Report, Prepared by the National White Collar Crime Center and the Federal Bureau of Investigation, January 1, 2004 -December 31, 2004. .

(3) عبد الفتاح بيومي حجازي، "حماية المستهلك من الغش التجاري والتقليد في عقود التجارة الإلكترونية عبر الإنترنت"، الندوة الثالثة لمكافحة الغش التجاري والتقليد في دول مجلس التعاون لدول الخليج العربية، الرياض، أيلول 2004، ص4.

ووفقا للسمات المميزة للتجارة الإلكترونية 1[(*)]، نجد أن المستهلك المتعامل مع هذا النمط من المعاملات الإلكترونية يكون معرضا- أكثر من غيره- للوقوع فريسة لعمليات النصب و الاحتيال التى قد تقع فى مجال الفضاء السيبيرى، وتعد الجرائم الواقعة على التجارة الالكترونية من أحدث الجرائم المعلوماتية.

وقد تناول المشرع الإماراتي هذا النوع من الجرائم في المادة 399 من قانون العقوبات 03/ 1987:

"يعاقب بالحبس أو بالغرامة كل من توصل إلى الاستيلاء لنفسه أو لغيره على مال منقول أو سند أو توقيع هذا السند أو إلى إلغائه أو إتلافه أو تعديله وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو صفة غير صحيحة متى كان من شأن ذلك خداع المجني عليه وحمله على التسليم". ويتعين أن يترتب على أفعال الاحتيال قيام الجاني بالاستيلاء على أموال الغير دون وجه حق وذلك باستخدام الحاسب الآلي بوصفه أداة إيجابية في هذا الاستيلاء.[(2)]

ولا يمكن حصر صور النصب والإحتيال فى التجارة الإلكترونية، ولكن يمكن أن نذكر عدد منها، مثلا[(3)]:

- عدم الوفاء بالسلعة المتعاقد عليها بالرغم من سداد المستهلك لثمنها.

(*) تتسم التجارة الإلكترونية بعدة خصائص وأهمها: عدم وجود علاقة مباشرة بين طرفى العقد، عدم الإعتماد على الوثائق الكتابية فى التعامل، تجاوز الحدود الزمنية و الجغرافية، اتساع مجال التجارة الإلكترونية، فكرة النشاط التجارى.

أنظر: محمد سامي الشوا، ثورة المعلومات، دار النهضة العربية، القاهرة، 2000، ص133.

(2) محمد محرم محمد علي، جريمة النصب والتجارة الإلكترونية، الموقع: www.omanlover.org/...

(3) جريمة النصب الواقعة على المتعاملين فى التجارة الإلكترونية، مقالة منشورة على الموقع: http://kenanaonline.com/.

- انتحال اسم أحد مواقع التسويق الشهيرة أو مواقع المنتجات الشهيرة والقيام بإنشاء موقع مماثل له.
- الترويج لسلعة مقلدة شبيهة بمنتج أصلى غالي الثمن والجودة، والتعدى على حقوق الملكية الفكرية لمنتج.
- الترويج لسلع غير معروفة باستخدام الإعلان الكاذب أو المضلل[**].

2-3- أشكال الاعتداء على تعاملات التجارة الالكترونية:

تأخذ الاعتداءات الواقعة على تعاملات التجارة الالكترونية شكل جرائم تقع على المضمون أو تقع على الوسائل الالكترونية المستخدمة في التجارة الالكترونية، أو السطو على أرقام البيانات الائتمانية.

أ. جرائم تقع على المضمون: ومن أمثلة هذه الجرائم الاعتداء على التوقيع الالكتروني، والتوقيع الالكتروني هو وسيلة يعبر بها شخص ما عن إرادته في الالتزام بتصرف قانوني معين، وقد عرّفه القانون الاتحادي الأمريكي بأنه: " صوت أو رمز أو معالجة إلكترونية مرفقة أو متحدة بعقد أو بغيره من السجلات يتم تنفيذها أو إقرارها من شخص تتوافر لديه نية التوقيع على السجل".

وليعتد به يجب أن يكون مقروءا إذا كان بالإمضاء ومرئيا، وهو لن يكون كذلك إلا إذا وضع على مستند مادي أيا كانت طبيعته ويترك أثرا واضحا، وأن يكون دائما أي أنه لا يزول مع الزمن[1].

(**) الكذب هو الإخبار عن شئ بخلاف ما هو عليه فى الواقع وهو يقوم على عنصرين أولا: مضمون زائف، ثانيا: قصد تزييف الحقيقة، أما الإعلان المضلل فهو الذى يكون من شأنه خداع المستهلك فهو لا يذكر بيانات كاذبة بل يصاغ فى عبارات تؤدى الى خداع المستهلك المتلقى.

(1) محمد عبيد الكعبي، مرجع سبق ذكره، ص235.

ويأخذ التوقيع الإلكتروني أشكالاً متعددة، ومن أهم صور الاعتداء عليه: التزوير أو التقليد، الدخول غير المشروع على أنظمة معلوماتية أو قواعد بيانات خاصة بالتوقيع الإلكتروني.

ب. جرائم تقع على الوسائل الالكترونية المستخدمة في التجارة الالكترونية، مثل الاعتداء على حقول الإنترنت:

وحقول الإنترنت أو ما يطلق عليها الشبكة العنكبوتية أو نظام الويب العالمي هي أكثر أقسام الإنترنت تطورا واستخداما، وتعرّف بأنها "مجموعة مصادر للمعلومات متضمنة في وثائق متمركزة في الحاسبات والشبكات حول العالم"[1]. وترتكز على بروتوكول HTTP. ونظرا لما لحقول الإنترنت وعناوينها من أهمية، باتت محلا للكثير من الاعتداءات غير المشروعة التي أصبحت تشكل خطرا عليها وعلى أسمائها، ومنها[2]: تدمير المواقع، تشويه المواقع Defacement، حجب الخدمة Denial of Service (DOS)، المحاكة والاختلاس والتضليل.

ج. السطو على أرقام البطاقات الائتمانية: البطاقة الائتمانية Credit Card عبارة عن بطاقة بلاستيكية تصدر عن بنك أو مؤسسة لتقديم خدمات أو تسهيلات معينة، على أن يقوم حاملها بسداد المبالغ المستحقة كليا أو جزئيا وفق نصوص العقد بين العميل (حامل البطاقة) والمصرف أو المؤسسة المصدرة للبطاقة[3].

---

(1) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ندوة تأثير محركات البحث عن إدارة الإنترنت، المنظمة العربية للتنمية الإدارية، الإسكندرية 31 يوليو-4 أغسطس 2005، ص47.

(2) محمد الألفي، أنماط جرائم الإنترنت، متاح على الموقع: www.eastlaws.com.

(3) هشام مفيد محمود، الآثار السلبية الناجمة عن تزوير البطاقات الائتمانية، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2002، ص107.

وتوجد عدة طرق وأساليب يتمكن قراصنة الحاسب الآلي والانترنت خلالها من الحصول على أرقام وبيانات البطاقات الائتمانية، وبالتالي استعمالها بصورة غير مشروعة، من أشهرها[1]: الاختراق غير المشروع لمنظومة خطوط الاتصالات العالمية، الاستدراج أو الصيد، تقنية تفجير الموقع المستهدف، أسلوب الخداع، تخليق أرقام البطاقات الائتمانية Card Math. ولتحقق جريمة الاستيلاء على أرقام بطاقات الائتمان فإنه يشترط توافر ركنين: الأول مادي يتمثل في سلوك ونتيجة ورابطة سببية والثاني ركن معنوي[2].

4- الآثار والمخاطر الناجمة عن الجرائم الواقعة على التجارة الالكترونية:

في الواقع لا توجد آليات واضحة لقياس الآثار الاقتصادية الناجمة عن جرائم الانترنت، وتوجد محاولات عدة من المؤسسات العامة والخاصة لقياس الآثار المباشرة وغير المباشرة لها، حيث من الصعب قياس الضرر الناجم من استخدام البرمجيات الخبيثة على الأفراد والمؤسسات. وتختلف هذه الآثار بحسب نوع الجريمة ونوع الأنظمة المعلوماتية أو بحسب أهمية البيانات المستهدفة.

فقد تكون الخسائر الاقتصادية لهذه الجرائم مباشرة مرتبطة بالضرر الاقتصادي المباشر ويخص قيمة التجهيزات والبرمجيات، موضوع الجريمة، وهو أقلها من حيث الأثر المالي، أو غير مباشرة، ناجمة عن توقف هذه المنظومات عن العمل مثلا: اختراق وتعطيل العمل بمنظومة شركة طيران، فبالرغم من عدم وجود أثر مالي مباشر، إلا أن

---

(1) عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الالكترونية، دار الفكر الجامعي، الإسكندرية، 2003، ص303.

(2) حسين بن سعيد بن سيف الغافري، الجرائم الواقعة على التجارة الإلكترونية، الموقع: www.mohamoon.com.

توقف المنظومة عن العمل يؤدي لخسائر كبيرة، أو تعطيل منظومة سوق الأوراق المالية لمدة دقائق قد ينجم عنه خسائر مالية تُقدر بعشرات آلاف الدولارات، أو بسرقة الأموال الالكترونية واستخدام الشبكة للاستيلاء على أموال الغير[1].

وتتحمل الدول خسائر فادحة تصل إلي مليارات الدولارات جراء انتشار جرائم التجارة الالكترونية، فوفقاً لتقرير مركز الدراسات الاستراتيجية والدولية CSIS عام 2014، فإن هذه الجرائم تُكلّف الاقتصاد العالمي حوالي 445 مليار دولار سنوياً[2]. بينما قدرت دراسة لإحدى الشركات المتخصصة حجم الخسائر من الجرائم الإلكترونية للعام 2014 ما بين 100 إلى 500 مليار دولار.

وهذا النطاق الواسع جدا في تقدير حجم الخسائر المترتبة على الجرائم الإلكترونية في العالم يدل على نقص حاد في المعلومات لقياسها، في حين نفتقر في الإمارات ودول الخليج العربي والوطن العربي برمته لقياس أو تقدير لحجم الخسائر الناجمة عن الجريمة الإلكترونية[3].

ويعد الهجوم الإلكتروني الذي تعرضت له شبكة حواسيب شركة سوني بيكتشرز إنترتينمتن بالولايات المتحدة أواخر نوفمبر/ تشرين الثاني 2014 أحدث أنواع الجرائم الإلكترونية، حيث كبدها خسائر مالية فادحة نجمت عن تسريب أفلام لم تكن عرضت في دور السينما، وسرقة مئات آلاف البيانات والرسائل إلى جانب تعطل أعمال الشركة فترة من الوقت.

(1) فاديا سليمان، مرجع سبق ذكره، ص10.

(2) 445 مليار دولار خسائر الاقتصاد العالمي من الجرائم الإلكترونية سنويا، مجلة الخزينة العمانية، نشر في 15 أبريل 2015، متاح على الموقع: http://www.alkhazinah.com/ar/445.

(3) رباب جبارة، مؤتمر الاقتصاد الإلكتروني يواصل جلساته في رأس الخيمة، "500 مليار دولار خسائر العالم من جرائم الإنترنت"، جريدة البيان الاقتصادي بتاريخ: 16/ 03/ 2015م.

وهناك عدة أسباب وراء تفشي الجريمة الإلكترونية وتهديدها السلبي على الاقتصاد، وأهمها:

1) جهل الناس بأنواع الجرائم الإلكترونية وطرق استدراج الضحايا.
2) ثقة الناس ببعض الأشخاص والمواقع والرسائل الإلكترونية دون التأكد من المصداقية.
3) تنوع طرق الجريمة الالكترونية وتعدد أساليبها مع تقدم الزمن وتطور التقنية الحديثة.
4) ضعف الوعي والمعرفة بأبعاد وتكاليف الجريمة الإلكترونية.
5) عدم حرص المستخدم على وضع برامج حماية ضد الفيروسات والتجسس أوعدم تحديث أنظمتها
6) نقص وضعف التشريعات وقوانين تخص هذا النوع من الجرائم مما أسهم في تمادي المجرمين.

ونظرا لما للاعتداء الواقع على التجارة الإلكترونية من أثر سيء على الاقتصاد العالمي، والكم الهائل للخسائر ووجود توقعات قوية بتزايد نسبة هذه الجرائم وتطور طرقها وتعدد مجالاتها وتفاقم حجم أضرارها، فإن ذلك يستدعي التصدي لها بقوة وبشتى الوسائل، ويمكن اعتماد طريقتين لذلك:

1- طريقة الاستدلال وتتضمن كل من التفتيش والمعاينة والخبرة، وهي تثير إشكالات إجرائية تعود لخصوصية الجريمة المرتكبة عبر الانترنت، إضافة للاستجواب والمواجهة وسماع الشهود.
2- الجهود الدولية والداخلية لتجسيد منظومة قانونية للوقاية من هذه الجرائم المستحدثة.

ولا يقتصر تأثير هذه الظّاهرة سلباً على الشّركات المتضـرّرة فقط، بل يتعدّاه ليؤثّر على حياة المستهلك والتّاجر والاقتصاد الوطني، وأيضا على الاستثمارات الأجنبية بشكلٍ خاص ومنظومة التّقدم التّكنولوجي بشكلٍ عام.

ثانيا: تطور التجارة الالكترونية بالإمارات وتزايد مخاطر الجرائم المعلوماتية

عرفت التجارة الالكترونية بدولة الامارات تطورا كبيرا، تلازما مع الطفرة الهائلة لتكنولوجيا الاتصالات والمعلومات، وبشكل أصبح فيه الأمن المعلوماتي مُهدداً بأساليب إجرامية متنوعة.

1- واقع التجارة الالكترونية بدولة الإمارات العربية المتحدة:

يشهد قطاع التجارة الإلكترونية بدولة الإمارات ثورة تنموية حقيقية، مما جعله يسهم في الدفع بعجلة التنمية الاقتصادية وتعزيز التنافسية الوطنية، فما هو واقع التجارة الالكترونية بدولة الإمارات؟

1-1- المكانة الاقتصادية لدولة الإمارات العربية المتحدة:

تعتبر الإمارات العربية المتحدة (*) جزءاً هاماً وفاعلاً في محيطها العالمي بحكم ثقلها الإقليمي والعربي والدولي وموقعها الاستراتيجي وعلاقاتها الاقتصادية والتجارية والاستثمارية، وما لديها من موارد إستراتيجية هامة وما تمتلكه من فوائض مالية مؤثرة. فهي تعد من أغنى الدول في المنطقة، وأعلاها من حيث الناتج المحلي الإجمالي، وقد

(*) تقع دولة الإمارات العربية المتحدة جنوب شرق الجزيرة العربية، وقد أعلن عن قيامها في 02 ديسمبر 1971، وتضم 7 إمارات هي: أبو ظبي ودبي والشارقة وعجمان ورأس الخيمة والفجيرة وأم القيوين. وتبلغ مساحتها 77.000كلم^2، نظام الحكم ملكي دستوري. وهي عضو بجامعة الدول العربية، ومنظمة المؤتمر الإسلامي، ومنظمتي أوبك والتجارة العالميتين. تضاعف عدد سكانها من 4.1 مليون نسمة عام 2005 إلى 8.4 مليون نسمة عام 2011.
أنظر: وزارة الاقتصاد، التقرير الاقتصادي السنوي لعام 2013، الإصدار 21، الإمارات العربية المتحدة، ص60.

تمكن الاقتصاد الإماراتي خلال الفترة (05-2010) من تحقيق نسب نمو موجبة، وصلت عام 2010 إلى.10 1 بالأسعار الجارية.[1]

وواصل اقتصاد دولة الإمارات نموه بوتيرة متسارعة، حيث بلغ الناتج المحلي الحقيقي نحو 1.1 تريليون درهماً سنة 2013م، وبنسبة نمو حقيقية جيدة بلغت 5.2٪ مقارنة بسنة 2012م، وأسهم في هذا التطور تزايد ناتج لقطاعات غير نفطية إلى حدود 731.8 مليار درهم عام 2013م وبنسبة نمو بلغت 5.4٪ مقارنة ب2012م. مما انعكس على ارتفاع حجم الاستهلاك النهائي والذي وصل لحدود 698.1 مليار درهم في2013م وبنسبة نمو10.7% مقارنة بسنة 2012.

وقد بلغت تجارة دولة الإمارات العربية المتحدة السلعية خلال عام 2013 نحو2.2 تريليون درهماً (610 مليار دولاراً)، وبنسبة نمو 15.78% مقارنة بسنة 2012م. وبحسب تصنيف منظمة التجارة العالمية لعام 2013م فقد تقدمت دولة الامارات العربية المتحدة إلى المرتبة 17 عالميا ضمن أكثر البلدان تصديرا في العالم، وذلك مقارنة بالمرتبة 18 في تقرير عام 2012م والمرتبة 20 عالميا في تقرير العام 2011م.[2]

وكان لنمو التجارة الخارجية آثار ايجابية على قطاع التجارة الالكترونية بدولة الإمارات.

2-1- حجم التجارة الالكترونية بدولة الإمارات:

بلغت عائدات التجارة الإلكترونية في العالم 1.5 تريليون $ سنة 2013، نصيب

---

(1) وزارة الاقتصاد، تقرير التطورات الاقتصادية والاجتماعية بدولة الإمارات العربية المتحدة 2005–2010، الإمارات العربية المتحدة، 2012، ص7.

(2) وزارة الاقتصاد، التقرير الاقتصادي السنوي للعام 2014، الاصدار 22، الامارات العربية المتحدة، ص25.

الدول العربية منها لا يتعدى 14 مليارا، بواقع أقل من 1% من حجم التجارة الإلكترونية. وتتصدر الصين العالم من حيث حجم التجارة بين المؤسسات التجارية والمستهلكين تليها الولايات المتحدة ثم الهند والبرازيل[1].

وتصدرت الإمارات أسواق المنطقة عام 2012 بعائد قدره 2.9 مليار دولار أميركي (10.7 مليار درهم)، لتحل أولا وتستحوذ على 32٪ من إجمالي سوق التجارة الإلكترونية في الشرق الأوسط تليها السعودية بـ 11%.

وأوضح تقرير صادر عن غرفة تجارة وصناعة دبي أن نمو سوق التجارة الإلكترونية بالإمارات يأتي مدعوماً بارتفاع الطلب وانتشار استخدام الإنترنت بنحو 2ر93٪ في الدولة خلال 2014م، ويعد من بين أعلى المعدلات في العالم العربي. كما توقع تقرير اقتصادي ارتفاع حجم التجارة الالكترونية للامارات بحلول عام 2018 الـ10 مليارات دولار بمعدل سنوي تراكمي نسبته 32٪.[2]

وانعكس تطور سوق التجارة الالكترونية بالإمارات على حجم الاستثمار في الإنترنت والتكنولوجيا، فحسب تقرير لبوابة الأعمال التجارية عبر الإنترنت "سندباد للأعمال"، فإن دولة الإمارات اجتذبت ما يقرب من نصف إجمالي استثمارات الشركات الناشئة في مجال الإنترنت والتكنولوجيا بمنطقة الشرق الأوسط وشمال إفريقيا، وتجاوز المبلغ 74 مليون دولاراً عامي 2011م و2012م، أي أكثر من مجموع تدفق الاستثمار للأردن والمملكة العربية السعودية ومصر ولبنان والمغرب مجتمعة.[3]

---

(1) التجارة الالكترونية في العالم الى أين ؟، صحيفة السوداني، الأحد 29 مارس 2015.

(2) توقعات بنمو سوق التجارة الالكترونية في الامارات بنسبة 32٪ سنوياً، موقع وكالة الانباء اليمنية: http://m.nbaonline-ye.com/read-69140.html

(3) الشركات الناشئة بالإمارات العربية المتحدة على المسار السريع لتحقيق نمو هائل، الموقع: http://www.tech-wd.com/wd/2013/06/08/startups-in-uae.

2- مؤهلات وفرص تطوير التجارة الالكترونية بدولة الإمارات:

هناك العديد من الفرص والمؤهلات تدعم ارتقاء دولة الامارات بالتجارة الالكترونية، ومن أهمها:

1- المكانة المتقدمة للإمارات في اقتصاد المعرفة والتنافسية، فقد أدركت القيادة الحكيمة لدولة الإمارات ضرورة منافسة الدول الرائدة في العالم على أساس رأس المال المعرفي، وانعكس ذلك على ترتيبها المتقدم في مختلف التقارير العالمية، مثلما يوضحه الجدول التالي:

الجدول رقم 02: ترتيب دولة الإمارات في بعض التقارير العالمية

اسم التقرير		الترتيب عالمياً	الترتيب عربياً	تاريخ التقرير
تقرير التنافسية العالمي	WORLD ECONOMIC FORUM	▲ 12	▲1	2014
تقرير تكنولوجيا المعلومات العالمي	WORLD ECONOMIC FORUM	▲ 23	▲1	2014
تقرير ممارسة أنشطة الأعمال	THE WORLD BANK	▲ 22	▲1	2014
تقرير تنافسية السياحة والسفر	WORLD ECONOMIC FORUM	▲ 24	▲1	2014
مؤشر الإبتكار العالمي	INSEAD The Business School for the World	▲ 36	–1	2014
تقرير التنمية البشرية العالمي	UNDP	▲ 40	–3	2014
تقرير مؤشر الإزدهـــار	LEGATUM INSTITUTE	▲ 28	–1	2013
تقرير تمكين التجارة العالمي	WORLD ECONOMIC FORUM	▲ 16	–1	2014

المصدر: مجلس الامارات للتنافسية ECC، الموقع:

http://www.ecc.ae/ar/competitiveness-ar/uae-ranking

ولقد ساهمت هذه الانجازات والنمو المتسارع في تحويل دولة الإمارات إلى دولة حديثة ومتطورة، فهي تتصدر المنطقة في جذب المواهب بتصنيفها في المرتبة الـ19 عالمياً، وذلك بفضل قدراتها التنافسية.

2- وجود رؤى إستراتيجية للارتقاء بتنافسية دولة الامارات، ومن أهمها: رؤية دولة الإمارات العربية المتحدة 2021م، استراتيجيه الحكومة الإلكترونية لدولة الإمارات العربية المتحدة (12-2014) الخطة الإستراتيجية لحكومة أبو ظبي2030 والخطة الإستراتيجية لحكومة دبي 2015م.

3- التطور الكبير في قطاع الاتصالات وتقنية المعلومات، حيث كشفت دراسة أعدتها كلية محمد بن راشد للإدارة الحكومية، بعنوان:" نظرة على الإعلام الاجتماعي في دولة الإمارات العربية المتحدة 2014م"، عن الحجم الكبير الذي تحتله هذه التقنيات في الدولة، إذ استطاعت الإمارات المحافظة على موقعها في صدارة دول المنطقة في استخدام مواقع التواصل الاجتماعي لأربع سنوات على التوالي، حيث تضاعف عدد مستخدمي " الفيسبوك " بالإمارات من 1,6 مليون مستخدم عام 2010م، إلى 5 ملايين مستخدم في عام 2014م، كما تزايد استخدام الهواتف الذكية، لتشكل ما نسبته 61٪ من إجمالي الهواتف المسجلة في الدولة. وتعد الإمارات ثاني أكبر أسواق التجارة الإلكترونية العالمية عبر استخدام الهواتف الذكية، وفقاً لدراسة أجرتها شركتا " بايبال PayPal - وإبسوس"«Ipsos -، التي أوضحت أن 57٪ من المتسوقين عبر الإنترنت اشتروا باستخدام الهواتف الذكية[1]. كما تتصدر الإمارات الدول العربية في عدد مستخدمي شبكة الإنترنت، حيث بلغ عدد المشتركين في الدولة عام 2013 حوالي7.8 ملايين مستخدم من أصل 9.3 ملايين عدد سكان الدولة، وفق تقرير صادر عن الأمم المتحدة في2014، وتبلغ نسبة مستخدمي الهواتف المتحركة بالإمارات 180 إلى 200٪، بمعدل يصل إلى جهازين أو خطين لكل شخص.[2]

(1) الوعي المجتمعي في مواجهة الجرائم الإلكترونية، جريدة الاتحاد الاماراتية، تاريخ النشر: الثلاثاء 17 مارس 2015.

(2) رباب جبارة، مرجع سبق ذكره.

4- ارتفاع متوسط دخل الفرد وظهور جيل جديد من المستهلكين والمتسوقين، فدخل الفرد الاماراتي من أكبر متوسطات الدخل في العالم، وبلغ متوسط نصيب الفرد من الناتج الثابت (بأسعار 2007) نحو 33 ألف دولار عام 2012م، وتصل نسبة الإنفاق الاستهلاكي الخاص إلى حوالي 60٪ من الناتج المحلي(1).

وتتزامن هذه الزيادة مع ظهور جيل جديد من المستهلكين "المستهلك الإلكتروني"، والذي يحمل معه دائماً جهازاً متصلاً بشبكة الإنترنت، وجيل جديد من المتسوقين يتعامل مع التجارة الإلكترونية من خلال أجهزة محمولة وشبكات التواصل الاجتماعي، دوافعهم لذلك الملاءمة لـ26٪ من الحالات وانخفاض الأسعار في 18٪ من الحالات وتنوع المنتجات والعروض لباقي الحالات.(2)

5- تطور نصيب التجارة الخارجية من الالكترونيات، فوفقاً لبيانات جمارك دبي بلغت قيمة الواردات من الإلكترونيات خلال الربع الأول من عام 2013م حوالي 28 ملياراً، فيما بلغت الصادرات وإعادة التصدير في الفترة نفسها حوالي 23 مليار درهم. وشكّلت الواردات من الصين أكثر من 45٪ من إجمالي واردات دبي للإلكترونيات ومستلزماتها خلال الربع الأول من 2012 حيث بلغت 13 مليار درهماً، وبلغت الواردات من ماليزيا نسبة 7٪، تلتها فيتنام بنسبة 4.5٪، والمجر بنسبة 7.4٪، وكوريا الجنوبية بأكثر من 4٪.(3)

6- التطور الحاصل في البنى التحتية، فقد أشار مؤشر التجارة الإلكترونية الذي

---

(1) وزارة الاقتصاد، التقرير الاقتصادي السنوي للعام 2013، الإصدار الحدي والعشرون، الإمارات العربية المتحدة، ص67.

(2) عبد الرحيم الطويل، الشرق الأوسط.. منجم الكتروني من ذهب، صحيفة البيان، 28 سبتمبر 2013، الموقع: http://www.albayan.ae/economy/local-market/2013-09-28-1.1968484.

(3) محمد الجداوي، 60 ٪ من التجارة الإلكترونية الخليجية من نصيب الإمارات، تقارير عربية، 11/ 10/ 2012، الموقع: http://elsokelarabia.net/?p=7053 .

أعلنت عنه شركة آي تـي كيرنـي» إلى حصـول الإمـارات علـى معـدل 100٪ في تأسيس البنية التحتية على الإنترنت، ومعدل 77٪ من القوانين والأنظمة الرقميـة، و49٪ في تطوير تجـارة التجزئـة، ليبلـغ مجمـوع معـدلها 50٪ في 2012م، وبـذلك تقدمت على دول مثل ماليزيا والإكوادور، وتركيا وعمان، في الوقت الذي حلـت فيه الصين أولاً، تلتها البرازيل.

7- زيادة الإنفاق عبر الانترنت، حيث تضم الإمارات أكبر سوق للتجارة الالكترونية في الشرق الأوسط، وبلغ إنفاق المستهلكين على الشـراء الالكترونـي لسـنة 2012 نحو 2.9 مليار دولاراً، تلتها السعودية ب1 مليار دولاراً، ثم قطـر ب 700 مليـون دولاراً. وتحتل المواقع المتخصصة في الموضـة والتكنولوجيـا أولى قنـوات الإنفـاق الإلكتروني.

8- نمـو عمليـات الـدفع عـبر البطاقـات، وبنسـبة 20٪ خـلال الربـع الأول مـن العام 2013م، مقارنة بالفترة نفسها من عام 2012 في الوقـت الـذي تجـاوزت فيـه المدفوعات عبر هذه البطاقات عام 2012 إلى 100 مليار درهـم، علمـا بأنهـا تمثـل مابين 10٪ و15٪ من إجمالي عمليات الدفع بالإمارات ويعـود تسـارع وتـيرة نمـو المدفوعات عبر البطاقات محليا إلى انتعاش قطاعي السياحة والتجزئة.[1]

9- تزايد الثقة بالتجارة الإلكترونية المحلية في الإمارات، بعدما كان المتسوقون يشترون من مواقع إلكترونية أجنبية، ولم تكن لديهم أسـباب قويـة أو فـرص للشـراء مـن مواقع إلكترونية محلية أو إقليمية نظراً لقلة الخيارات وانخفـاض الجـودة.، وحاليـا تحول شعورهم باتجاه المواقع الالكترونية المحلية.

10- إطلاق مبادرات لتطوير قطاع التجارة الالكترونيـة: ومـن بـين هـذه المبـادرات:

(1) مدي سعد، الإمارات الأولى إقليمياً والسادسة عالمياً في التجارة الإلكترونية، الموقع :
http://www.alkhaleej.ae/portal/686aec3e-f8e7-4fc6-bf54-24770b806ab0.aspx

مبادرة "بوابة الدفع الإلكتروني، مبادرة "الحكومة الذكية "(*)، ليستفيد أفراد المجتمع من خدماتها عبر الهواتف النقالة الذكية طوال ال 24 ساعة يوميا خلال كامل أيام الأسبوع، وطوال أيام السنة (1).

11- تحرير قطاع الاتصالات، حيث كانت مؤسسة الإمارات للاتصالات "اتصالات www.etisalat.ae" تحتكر تقديم خدمات الإنترنت من خلال وحدة "الإمارات للانترنت والوسائط المتعددة" منذ إنشائها في: 7 مارس 2000م، وبعد أن توصلت دراسة شاملة بأن أبرز عائق أمام انتشار التجارة الالكترونية هو عدم الثقة بمستوى الأمان في شبكة الانترنت، أسندت مهمة التجارة الالكترونية في الإمارات إلى مؤسسة الإمارات للاتصالات كمؤسسة قطاع خاص،

والتي أطلقت مشروع (كومترست) كأول مشروع لتقديم خدمات التجارة الالكترونية الشاملة بالمنطقة، وبذلك تكون دولة الإمارات قد تجاوبت مع المبادئ التوجيهية العالمية في خوصصة هذا النشاط، وتجاوبت مع مفاتيح تطوره وفي مقدمتها توفير الثقة لدى أصحاب المشاريع والزبائن معا بشأن سلامة وأمن بيئة التجارة الالكترونية عند توليها من جهات تتوفر لها كفاءة تحمل المسؤولية القانونية عن سلامة الحلول المقررة في ميدان التجارة الالكترونية.(2)

(*) مبادرة الحكومة الذكية، أعلنها صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي وذلك في22 ماي 2013. بهدف تقديم الخدمات الحكومية عبر الهواتف على مستوى الدولة، تبلغ نحو 4000 خدمة، وهي مشروع إماراتي وطني، لا هو محلي ولا هو اتحادي، ويدخل ضمن رؤية الإمارات 2021. أنظر: جريدة الإمارات اليوم (صفحة محليات)، دبي، بتاريخ 23 ماي 2013.

(1) عبير عبد الحليم، "التحوّل نحو الحكومة الذكية وفق مبدأ الأولويات"، جريدة الإمارات اليوم، أبوظبي، 12 سبتمبر 2013،

(2) واقع التجارة الإلكترونية ومزاياها، الموقع: http://www.boosla.com/showArticle.php?.

3- تزايد مخاطر الجرائم المعلوماتية الواقعة على التجارة الالكترونية بالإمارات:

على الرغم من الانتشار الواسع لاستخدامات وسائل الاتصال الحديث ونظم التبادل الالكتروني واعتماد المؤسسات على النظم الحديثة في استخدام البيانات بدولة الإمارات، إلا أن الجرائم الالكترونية بها وبالرغم من تزايد معدلاتها لا ترتقي إلى درجة الظاهرة مقارنة بالدول الأخرى.

ففي أبو ظبي مثلا أفادت دائرة القضاء بأن النيابة استقبلت 140 قضية خلال عام 2012 تتعلق بجرائم إلكترونية متنوعة ما بين احتيال ونصب، وفي عام 2011 تلقت شرطة دبي 549 بلاغاً عن الجرائم الإلكترونية.

فوفقا للموقع الالكتروني لهيئة الامارات للهوية، بلغت خسائر دولة الامارات في عام 2012 حوالي 420 مليون دولاراً بسبب الجرائم الالكترونية، ووفقا لمصادر أجنبية بلغت تكلفة هذه الجرائم بالسعودية 2,6 مليار دولاراً عام 2013 بينما أظهرت إحصائية أجرتها FBI حول الخسائر الناجمة عن جرائم الانترنت بأن الخسائر الاقتصادية للضرر الناجم عن البرمجيات بلغ نحو 17,5 مليار دولاراً في عام 2004 وانخفض إلى 13,3 ملياراً في عام 2006.[(1)]

وحيث أن شخصين على أقل تقدير من القاطنين بالإمارات يقعون ضحية للجرائم الإلكترونية في كل دقيقة بفعل الفيروسات ورسائل التحايل الإلكترونية وهجمات تصيّد المعلومات السرية والمصرفية وغيرها، أي أن أكثر من 1.4 مليون مستخدماً في الإمارات يتعرضون لهجمات إلكترونية يومياً.

ومن أكثر أشكال الجريمة الإلكترونية انتشاراً بالإمارات: الفيروسات أو البرمجيات الخبيثة التي تستهدف الحواسيب ومن السهل تجنبها ونسبتها 51٪، ورسائل الاحتيال الإلكترونية نسبتها 19٪، تليها هجمات تصيّد المعلومات الخاصة والسرية

(1) تكاتف الجهود العربية لمكافحة الجريمة الالكترونية وجرائم المعلوماتية وأثرها على العمليات المالية، موقع اتحاد المصارف العربية: http://www.uabonline.org/ar/magazine.

نسبتها 18٪. وتعتمد أنشطة الجريمة الإلكترونية على رسائل الاحتيال الإلكترونية وهجمات تصيّد المعلومات الخاصة والسرية لسرقة المعلومات المصرفية وبيانات البطاقات الائتمانية لاستغلالها في أغراض إجرامية.

ومن أهم الجرائم المذكورة في قانون مكافحة جرائم تقنية المعلومات، نجد: الدخول غير المشروع، وتزوير المستندات، وإعاقة الوصول إلى الخدمة أو الدخول إلى الأجهزة والبرامج، وإدخال ما من شأنه إيقاف الشبكة عن العمل أو تعطيلها، والتنصت والالتقاط، والاحتيال الإلكتروني[1]. ولمواجهة هذا الانتشار للجرائم الالكترونية، تبنت دولة الإمارات استراتيجية شاملة للتصدي لها.

ثالثا: استراتيجيه الإمارات في التصدي للجرائم الواقعة على التجارة الالكترونية

في مقابل الفرص الواعدة التي تنتظر قطاع التجارة الإلكترونية بدولة الإمارات، يواجه هذا القطاع تهديدات مستمرة جراء انتشار الجرائم الإلكترونية، واختراق بطاقات الائتمان وتزايد تكاليف ذلك. والتزاما من القيادة الحكيمة لدولة الإمارات بتحقيق رؤية الحكومة 2021م، والمبنية على مواجهة التحديات واستغلال الفرص الواعدة أمامها، لتغيير اتجاه التنمية نحو اقتصاد المعرفة، تم تبني استراتيجيه[*] ترتكز على عدة خطوات وإجراءات عملية لمواجهة مخاطر جرائم التجارة الإلكترونية، وحماية

(1) المؤتمر الدولي الرابع لمكافحة جرائم تقنية المعلومات ليوم 14/ 12/ 2011م، موقع معهد التدريب والدراسات القضائية:
http://www.itjs.gov.ae/Report/ReportDesc.aspx?Con_ID=41&type=CN&MenuID=13&Catid=

(*) تعرف الإستراتيجية بأنها مجموعة الخيارات الطويلة الأجل التي يضعها مديرو البرامج في شكل خدمات وسياسات وخطط عمل. أنظر: فؤاد عبد المنعم البكري، التنمية السياحية، عالم الكتاب، الطبعة الأولى 2004، ص9.

النظام المالي للدولة، بالمشاركة والتعاون بين جميع الجهات المعنية كجهات إنفاذ القانون والمؤسسات المالية وغير المالية والتجارية والاقتصادية والجهات الحكومية، مع تثمين الدور الإعلامي في هذا المجال، وذلك باعتماد العديد من الخطوات والاجراءات، مست الجوانب التاليـة:

1- تنظيم وتحديث التشريعات:

إن المهتم بالإطار القانوني للتجارة الإلكترونية في الإمارات، سيطلع أساسا على القوانين التالية:

1) القانون الاتحادي رقم 1/ 2006 في شأن المعاملات والتجارة الإلكترونية.

2) القانون الاتحادي رقم 2/ 2006 والمتعلق بمكافحة جرائم تقنية المعلومات.

3) قرار مجلس الوزراء رقم 21/ 2013 بشأن لائحة أمن المعلومات في الجهات الاتحادية.

4) مرسوم بقانون إتحادي رقم 05/ 2012 في شأن مكافحه جرائم تقنية المعلومات.

5) مرسوم بقانون اتحادي رقم 03/ 2012 بإنشاء الهيئة الوطنية للأمن الالكتروني.

6) القانون الصادر بإمارة دبي، وهو: القانون رقم 2/ 2002 بشأن المعاملات الإلكترونية.

وتعد دولة الإمارات العربية المتحدة من أوائل الدول العربية التي أصدرت قانوناً مختصاً في مكافحة جرائم المعلومات، حيث أصدر صاحب السمو الشيخ خليفة بن زايد آل نهيان رئيس الدولة، القانون الاتحادي رقم 2/ 2006 والمتعلق بمكافحة جرائم تقنية المعلومات، ويهدف القانون إلى ما يلي:

1) حماية هذه التقنية الجديدة من أي استغلال لها يشكل اعتداءاً على الحقوق والحريات المقررة.

2) الوصول إلى نظام قضائي فعال وتشديد العقوبات على مرتكبي مثل هذه الجرائم.
3) كفالة حقوق المتعاملين إلكترونياً وتحديد التزاماتهم وتشجيع وتسهيل المعاملات الإلكترونية.
4) إزالة العوائق أمام التجارة الإلكترونية، وتعزيز ثقة المتعاملين في المعاملات والمراسلات الإلكترونية.
5) تأكيد أهمية اعتماد التوقيع الإلكتروني والمحرر الإلكتروني.

وقد شكل هذا القانون نواة لقانون استرشادي عربي للجرائم المعلوماتية سمي "قانون الإمارات العربي الاسترشادي لمكافحة جرائم المعلومات وما في حكمها" نسبة إلى الدولة التي أعدته(**).

وبالنسبة للانتهاكات التي تخص المواقع الإلكترونية وأسماءها تم تجريمها في المادة 14 من القانون 2/ 2006. كما تناول المشرع جريمة النصب والاحتيال في المادة 399 من قانون العقوبات.

إلا أن الواقع العملي أثبت قصور القانون في مواكبة التطورات السريعة والمخاطر التي نتجت عن التقدم المذهل في وسائل التقنية الحديثة، وظهور نوعية معينة من الجرائم لم يتعرض لها القانون، مما استدعى استبداله بالمرسوم بالقانون الاتحادي 5/ 2012 (*)، والذي جاء مكملاً لما ورد في قانون العقوبات الاتحادي وبشكل ومواكب للتطورات العملية في مجال تقنية المعلومات.

(**) قانون الإمارات العربي الاسترشادي لمكافحة جرائم المعلومات وما في حكمها، اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم 495- 19- 8/ 10/ 2003، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417- د 21/ 2004. ويتكون من 27 مادة.

(*) المرسوم بقانون اتحادي رقم 05/ 2012 يتعلق بمكافحة جرائم تقنية المعلومات، يتكون من51
–

كما تم ووضع اللوائح والأنظمة والإجراءات التي تهدف للحد من مخاطر تلك الجرائم بالتزامن مع تدريب القائمين على إنفاذ القانون على مواجهة الجرائم الالكترونية وابتكار الحلول والأدوات التي من شأنها الكشف عنها وتعزيز التعاون الدولي والتبادل المشترك للمعلومات والخبرات بين الدول.[1]

2- تعزيز الإجراءات الأمنية في الشبكة المعلوماتية (الأمن المعلوماتي):

إن الإجراءات الأمنية المناسبة يمكن أن تساهم في ضمان النتائج المرجوة وتقلص اختراق المعلومات والتلاعب بها، وكانت شركة IBM الأمريكية أول من وضع تعريفاً لأمن المعلومات، وكانت تركز على حماية البيانات من حوادث التزوير، والتدمير أو الدخول غير المشروع على قواعد البيانات.

وترتيب دولة الإمارات في الجاهزية المعلوماتية 24 عالميا، ربما لم يجعلها في قائمة (20) دولة التي تواجه مخاطر خروق أمنية. وتبقى مسألة الأمن على الشبكة مصدر قلق لكل المتسوقين الإلكترونيين بالإمارات العربية المتحدة حسب تقرير شركة (PayPal)، سواء أكان ذلك على شكل احتيال في الدفع أم عدم التسليم أم التزوير، إذ اعتبر 40٪ من متسوقي الشرق الأوسط وشمال إفريقيا أن عامل الأمن يمثل مصدر قلق رئيسي.[2] ويعتبر المتسوقون في منطقة الشرق الأوسط وشمال أفريقيا أنّ الأمان هو مصدر القلق الرئيسي لديهم. وفيما تتسع بيئة التجارة الإلكترونية وتتغير في الشرق

=

مادة، أصدره صاحب السمو خليفة بن زايد آل نهيان رئيس الدولة، بتاريخ: 25 رمضان 1433هـ، الموافق لـ13 أغسطس 2012م. خصص المشرع نصوص المواد (من رقم 2 إلى رقم 39 منه) للجرائم التي تنص عليها، ويحتوي كل نص على جريمة واحدة أو أكثر.

(1) استراتيجيه إماراتية لمواجهة الجرائم الإلكترونية، البيان/ سياسة، 25/ 9/ 2013:
www.albayan.ae/across...uae/.

(2) عبد الرحيم الطويل، مرجع سبق ذكره.

الأوسط، تزيد الحاجة إلى حل بسيط وآمن للدفع من أجل الحصول على تجربة تسوق متعددة القنوات.

وتشير التقارير إلى أهمية سوق الإمارات الذي يعد الأفضل خليجيًا وإقليميًا في تطبيق نظم ومعايير أمن المعلومات واستخدام برمجيات وأنظمة الحماية الإلكترونية، نظرًا لارتفاع الوعي التقني فيها. وعلاوةً على ارتفاع الإنفاق السنوي المتنامي على المعلوماتية، يتوقع أن تبلغ نسبة النمو السنوي لإنفاق الإمارات على أمن المعلومات الرقمية 20٪ في الأعوام الخمسة حتى عام 2019م ليصل لمليار درهم في 2020م، وبذا تعد الإمارات الأعلى إنفاقاً على أمن المعلومات في الشرق الأوسط(1).

ومن ناحية أخرى تركز الإستراتيجية الأمنية للشرطة في الإمارات على الجانب الوقائي في مكافحة الجريمة وإقرار الأمن والاستقرار والسلامة العامة بين المواطنين والمقيمين مع التسلح بالخبرات اللازمة، وإنشاء إدارة الأدلة الإلكترونية ونظام الشرطي الإلكتروني وتدريب الكوادر الفنية للتصدي لهذا النوع من الجرائم عند وقوعها.

3- تشديد العقوبات:

نص القانون 2/ 2006م على اعتبار الجرم المعلوماتي كالجرم التقليدي، وعلى وجود عقوبات تقليدية تراوحت بين السجن المؤقت والغرامة التي لا تتجاوز مبلغ 2 مليون درهماً، بالإضافة لعقوبات تكميلية يجب الحكم بها، وهي مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجرائم، والإغلاق الكلي أو

(1) الإمارات تتصدر الشرق الأوسط فى الإنفاق على أنظمة الحماية الإلكترونية، صحيفة الخليج الجدد، نشر بتاريخ 06/ 12/ 2014م. الموقع: http://www.thenewkhalij.com/ar/node/6482.

لمدة معينة للمحل أو للموقع الذي يرتكب فيه أي من الجرائم بشرط توافر علم المالك، بالإضافة لعقوبة الإبعاد إذا كان المحكوم عليه أجنبيا وحكم عليه بالحبس.[1]

4- تثمين الجهود المحلية وتعزيز التعاون الدولي في مجال مكافحة الجريمة المعلوماتية:

إزاء انتشار الجرائم الإلكترونية كظاهرة عالمية، بات من الضروري إيجاد إطار فعال يضمن استحداث آليات للتعاون الدولي في مجال مكافحة هذه الجرائم، من خلال تشجيع تبادل الخبرات من أجل الضبط الجنائي لها، باعتبارها

جرائم افتراضية مع تكوين مختصين في المجال سواء الضبطية القضائية أو القضاء بوجه عام، وإيجاد تشريع دولي خاص لمواجهة هذا الخطر، والحرص على إدراج هذه الجرائم ضمن اختصاصات المحكمة الجنائية الدولية نظرا لطابعها العالمي. وتسهر دولة الإمارات على تعزيز جهود التعاون والتنسيق بين جهات إنفاذ القانون والمؤسسات المالية والتجارية والاقتصادية ذات الصلة، وتثمين جهودها في مجال مكافحة الجرائم الالكترونية.

وفي هذا الشأن توجد العديد من الاتفاقيات الدولية التي تنظم وتسهم في جعل الإمارات مقراً متميزاً لمواجهة هذا النوع من التحديات الإلكترونية. وهناك فريق عمل(انتربول) خاص وإقليمي لمواجهة الجرائم الإلكترونية، وفريق عمل دولي من أهدافه الإستراتيجية جعل الإنترنت مكاناً أكثر أمناً للمعاملات التجارية، ورصد المعتدين وحماية الضحايا، ويتكون من الجمارك والجنسية الأمريكية، شرطة الخيالة الملكية الكندية، مركز الأطفال المُستغلين في بريطانيا، شرطة البريد الإيطالية،

(1) ندوة جرائم تقنية المعلومات بين التحديات والحلول تضع نقاطا للحلول التقنية على حروف مخاطر الجرائم الإلكترونية، بتاريخ 10 يونيو2012، الموقع:
http://mogtamaa.telecentre.org/profiles/blogs/2487793:BlogPost:69404

(الانتربول) بأعضائه 180 دولة، (اليوروبول) الأوروبي، الشرطة الاسترالية الاتحادية والشرطة النيوزلندية، إضافة لوزارة الداخلية الإماراتية.[1]

5- **تكثيف الحملات الإعلامية والتوعية:**

تلعب وسائل الإعلام المختلفة دورا كبيرا في الحد من انتشار جرائم التجارة الالكترونية، وذلك من خلال نشر الوعي لدى أفراد المجتمع بخطورة تلك الجرائم وتثقيفهم كي لا يقعوا تحت طائلة القانون من خلال نشر الثقافة القانونية والتي اتخذتها دائرة القضاء بالإمارات شعاراً لها لعام 2013م.[2]

وتعدُّ دولة الإمارات سباقة في الإسهام بوضع تصورات لمكافحة كل أشكال الجرائم المستحدثة من خلال مشاركاتها واحتضانها للمؤتمرات والاجتماعات ذات الصلة بها، وتجلى ذلك في تبني جامعة الدول العربية القانون الاتحادي رقم 2/ 2006م لمكافحة جرائم تقنية المعلومات كقانون استرشادي.

وهناك تشديد على أهمية تكثيف حملات التوعية والتحذير من مخاطر الدخول غير المسؤول للمواقع المشبوهة أو التعامل الالكتروني مع شركات وأشخاص مجهولي الهوية قبل الوقوع في براثن الاحتيال الالكتروني داخل الدولة وخارجها، وذلك من خلال تكثيف اللقاءات العلمية والملتقيات.

---

(1) مركز الخليج للدراسات، الجرائم الإلكترونية عابرة للقارات سلاحها خبرة تقنية عالية، الموقع: http://www.alkhaleej.ae/portal/7104572e-26ff-4194-8051-dc1c84f902e7.aspx.

(2) استراتيجيه إماراتية لمواجهة الجرائم الإلكترونية، البيان/ سياسة، 25/ 9/ 2013: www.albayan.ae/across...uae/.

الخاتمة

تعد الجريمة المعلوماتية ظاهرة عالمية، ومصدر قلق عابر للحدود والقوميات، ومن أشهر هذه الجرائم، نجد جرائم النصب والاحتيال على الأموال المتداولة في المعاملات التجارية الالكترونية، وهي تحتاج إلى جهود واستراتيجيات دولية ومحلية لمواجهتها. ومن أهم النتائج التي توصلت لها الدراسة:

1) تأخذ الاعتداءات الواقعة على تعاملات التجارة الالكترونية شكل جرائم تقع على المضمون، أو تقع على الوسائل الالكترونية المستخدمة في التجارة الالكترونية أو السطو على أرقام البيانات الائتمانية.

2) للجرائم المعلوماتية الواقعة على التجارة الإلكترونية آثار مباشرة وغير مباشرة على الدول، مما يستدعي التصدي لها بقوة وبشتى الوسائل، إما بالاستدلال، أو من خلال جهود داخلية ودولية.

3) عرفت التجارة الالكترونية بالامارات تطورا كبيرا تلازما مع الطفرة الهائلة في مجال تكنولوجيا الاتصال والمعلومات، وبالشكل الذي أصبح فيه الأمن المعلوماتي مُهدداً بأساليب إجرامية متنوعة.

4) أكثر أشكال الجريمة الإلكترونية انتشاراً بالإمارات هي الفيروسات أو البرمجيات الخبيثة التي تستهدف الحواسيب ورسائل الاحتيال الإلكترونية، تليها هجمات تصيّد المعلومات الخاصة والسرية.

5) تبنت دولة الامارات استراتيجية شاملة لمواجهة المخاطر الناجمة عن جرائم التجارة الإلكترونية، ترتكز على: تنظيم وتحديث التشريعات، تعزيز الإجراءات الأمنية بالشبكة المعلوماتية، تشديد العقوبات، تثمين الجهود المحلية وتعزيز التعاون الدولي، تكثيف الحملات الإعلامية والتوعية.

وبناء على ما تم التوصل إليه من نتائج أوصت الدراسة بجملة من التوصيات، وهي:

1. اعتماد تدابير لزيادة وعي الجماهير والعاملين بالأجهزة القضائيّة وأجهزة انفاذ القوانين بأهمية مكافحة هذه الظاهرة.
2. ضرورة العمل على تدريب وتأهيل القائمين على مكافحة جرائم تقنية المعلومات في المؤسسات القانونية والقضائية والأمنية والخبراء والمحامين، والتأكيد على تشديد العقوبة نظرًا لخطورة هذه الجرائم.
3. التأكيد على تشديد العقوبة نظرًا لخطورة هذه الجرائم،
4. إنشاء مركز وطني مختص بجرائم تقنية المعلومات، له برنامج شامل يهدف للتوعية بالتشريعات والتطبيقات والتعاون بين مؤسسات المجتمع لمكافحة الجرائم الواقعة على التجارة الالكترونية.
5. التأكيد على استمرارية عقد المؤتمرات المتخصصة والندوات وورش العمل في مجال جرائم التجارة الالكترونية، بما لها من آثار ايجابية للوقوف على أحدث المستجدات في هذا المجال.
6. التأكيد على أهمية دور الأسرة والمؤسسات الدينية والتربوية والاجتماعية والإعلامية والجمعيات لبذل المزيد من الجهود، في مجال تسليط الضوء على خطورة هذه الجرائم، وطرق الوقاية منها.
7. زيادة مستوى التعاون العربي، وإصدار قوانين ونظم مشتركة لمواجهة الجرائم المعلوماتية للتجارة الالكترونية.

وأخيرا فإن نجاح أي إستراتيجية يتم اعتمادها لمواجهة الجرائم المعلوماتية الواقعة على التجارة الالكترونية لا يتوقف على الارتقاء بمستوى الوعي العام فحسب، بل يستوجب وجود كوادر بشرية مؤهلة قادرة على دعم ديناميكية سوق العمل أيضاً، الأمر الذي من شأنه الحد من معدلات البطالة.

ثبت المراجع

المراجع العربية:

1- رأفت رضوان، عالم التجارة الالكترونية، بحوث ودراسات، المنظمة العربية للتنمية الإدارية، 1999.

2- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، دار النهضة العربية، 2005.

3- محمد سامي الشوا، ثورة المعلومات، دار النهضة العربية، القاهرة، 2000.

4- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مطابع الهيئة المصرية العامة للكتاب، 2003.

5- عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الالكترونية، دار الفكر الجامعي، الإسكندرية، 2003.

6- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، 2006.

7- عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية العربية، جزء1، دار الفكر الجامعي، الإسكندرية، 2002.

8- فؤاد عبد المنعم البكري، التنمية السياحية، عالم الكتاب، الطبعة الأولى2004.

9- وزارة الاقتصاد، تقرير التطورات الاقتصادية والاجتماعية بدولة الإمارات العربية المتحدة 2005-2010، قطاع شؤون السياسات الاقتصاد، الإمارات العربية المتحدة، 2012.

10- وزارة الاقتصاد، التقرير الاقتصادي السنوي للعام 2013، الإصدار الحدي والعشرون، الإمارات العربية المتحدة.

11- وزارة الاقتصاد، التقرير الاقتصادي السنوي للعام 2014، الاصدار الثاني والعشرون، الامارات العربية المتحدة.

12- غازي عبد الرحمان هيان الرشيد، "الحماية القانونية من جرائم المعلوماتية (الحاسب والانترنت)"، أطروحة لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004.

13- أخام بن عودة زواوي مليكة، تحديات ظاهرة الجريمة العابرة للأوطان والثورة المعلوماتية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس/ ليبيا، 27-30 اكتوبر 2009.

14- عبد الفتاح بيومي حجازي، "حماية المستهلك من الغش التجاري والتقليد في عقود التجارة الإلكترونية عبر الإنترنت"، الندوة الثالثة لمكافحة الغش التجاري والتقليد في دول مجلس التعاون لدول الخليج العربية، الرياض، أيلول 2004.

15- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ندوة تأثير محركات البحث عن إدارة الإنترنت، المنظمة العربية للتنمية الإدارية، الإسكندرية 31 يوليو-4 أغسطس، 2005.

16- هشام مفيد محمود، الآثار السلبية الناجمة عن تزوير البطاقات الائتمانية، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2002.

17- ثناء أبا زيد، " واقع التجارة الإلكترونية والتحديات التي تواجهها عربياً ومحلياً"، مجلة جامعة تشرين للدراسات والبحوث العلمية، سلسلة العلوم الاقتصادية والقانونية، المجلد (27) العدد (4)، 2005.

18- رحاب فايز أحمد سيد، جرائم الكتب الإلكترونية: دراسة تحليلية لوضع استراتيجية حماية لها، مجلة اعلم (قيد النشر)، الاتحاد العربي للمكتبات والمعلومات، 2014.

19- فاديا سليمان، الجرائم المعلوماتية وأثرها على العمليات المالية والمصرفية، مجلة الدراسات المالية والمصرفية - العدد الاول لسنة 2015، الأكاديمية العربية للعلوم المالية والمصرفية، عمان، الأردن.

20- 445 مليار دولار خسائر الاقتصاد العالمي من الجرائم الإلكترونية سنويا، مجلة الخزينة العمانية، نشر في 15 أبريل 2015، متاح على الموقع:
http://www.alkhazinah.com/ar/445.

21- قانون المعاملات والتجارة الإلكترونية رقم 02/ 2002 بإمارة دبي، تاريخ النشر: 16-02-2002.

22- قانون الإمارات العربي الاسترشادي لمكافحة جرائم المعلومات وما في حكمها، القرار رقم 495- د19- 8/ 10/ 2003، مجلس وزراء العدل العرب في دورته التاسعة عشرة القرار.

23- المرسوم بقانون اتحادي رقم 05/ 2012 في شأن مكافحة جرائم تقنية المعلومات. بتاريخ: 13 أغسطس 2012م.

24- الإمارات تتصدر الشرق الأوسط فى الإنفاق على أنظمة الحماية الإلكترونية، صحيفة الخليج الجدد، نشر بتاريخ 06/ 12/ 2014م. الموقع:
http://www.thenewkhalij.com/ar/node/6482.

25- التجارة الالكترونية في العالم الى اين؟، صحيفة السوداني، الأحد، 29 مارس 2015.

26- الوعي المجتمعي في مواجهة الجرائم الإلكترونية، جريدة الاتحاد الاماراتية، تاريخ النشر: الثلاثاء 17 مارس 2015.

27- رباب جبارة، مؤتمر الاقتصاد الإلكتروني يواصل جلساته في رأس الخيمة، "500 مليار دولار خسائر العالم من جرائم الإنترنت"، جريدة البيان الاقتصادي بتاريخ: 16/ 03/ 2015م.

28- عبد الرحيم الطويل، الشرق الأوسط.. منجم الكتروني من ذهب، صحيفة البيان، 28 سبتمبر 2013، الموقع:
http://www.albayan.ae/economy/local-market/2013-09-28-1.1968484.

29- عبير عبد الحليم، " التحوّل نحو الحكومة الذكية وفق مبدأ الأولويات"، جريدة الإمارات اليوم، أبوظبي، 12 سبتمبر 2013،

30- المؤتمر الدولي الرابع لمكافحة جرائم تقنية المعلومات ليوم 14/ 12/ 2011م، موقع معهد التدريب والدراسات القضائية:
http://www.itjs.gov.ae/Report/ReportDesc.aspx?Con_ID=41&type=CN&MenuID=13&Catid=0&m

31- استراتيجيه إماراتية لمواجهة الجرائم الإلكترونية، البيان/ سياسة، 25/ 9/ 2013:
www.albayan.ae/across...uae/.

32- الشركات الناشئة بالإمارات العربية المتحدة على المسار السريع لتحقيق نمو هائل، الموقع: http://www.tech-wd.com/wd/2013/06/08/startups-in-uae.

33- تكاتف الجهود العربية لمكافحة الجريمة الالكترونية وجرائم المعلوماتية وأثرها على العمليات المالية، موقع اتحاد المصارف العربية:
http://www.uabonline.org/ar/magazine.

34- توقعات بنمو سوق التجارة الالكترونية في الامارات بنسبة 32٪سنوياً، موقع وكالة الانباء اليمينية:
http://m.nbaonline-ye.com/read-69140.html

35- حمدي سعد، الإمارات الأولى إقليمياً والسادسة عالمياً في التجارة الإلكترونية، الموقع:
http://www.alkhaleej.ae/portal/686aec3e-f8e7-4fc6-bf54-24770b806ab0.aspx.

36- جريمة النصب الواقعة على المتعاملين فى التجارة الإلكترونية، مقالة منشورة على الموقع: http://kenanaonline.com/users/ahmedkordy/posts/277940

37- حسين بن سعيد بن سيف الغافري، الجرائم الواقعة على التجـارة الإلكترونيـة، الموقع: www.mohamoon.com..

38- محمد محرم محمد علي، جريمة النصب والتجارة الإلكترونية، الموقع:
www.omanlover.org/...

39- محمد الألفي، أنماط جرائم الإنترنت، متاح على الموقع: www.eastlaws.com.

40- محمد الجداوي، 60٪ من التجارة الإلكترونية الخليجيـة مـن نصـيب الإمـارات، تقارير عربية، 11/ 10/ 2012، الموقع: http://elsokelarabia.net/?p=7053 .

41- مركز الخليج للدراسات، الجرائم الإلكترونية عابرة للقارات سلاحها خبرة تقنية عالية، الموقع: http://www.alkhaleej.ae/portal/7104572e-26ff-4194-8051-dc1c84f902e7.aspx

42- ندوة جرائم تقنية المعلومات بين التحديات والحلول تضع نقاطا للحلول التقنيـة على حروف مخاطر الجرائم الإلكترونية، بتاريخ 10 يونيو2012، الموقع:
http://mogtamaa.telecentre.org/profiles/blogs/2487793:BlogPost:69404.

43- واقع التجارة الإلكترونية ومزاياها، الموقع:
http://www.boosla.com/showArticle.php?.

المراجع الأجنبية:

44- David Icove, Karl Seger & William Von Storch, Computer Crime, a Crime Fighter's Handbook, New Jersey: Prentice Hall , August 1995.

45- Grabosky, P. Electronic Crime ,New Jersey: Prentice Hall, 2006.

46- Kurbalua Jovan , Gelbestein Eduardo ,Gouvernance de l'internet – enjeux , acteurs et factures , publie par diplofoundation et global knowledge partnership , Suisse , 2005.

47- Internet Fraud Complaint Center (IFCC) (2001), Six-Month Data

Trends Report, Prepared by the National White Collar Crime Center and the Federal Bureau of Investigation, May-November, 2000.

48 - Internet Fraud Complaint Center (2005), IC3 2004 Internet Fraud: Crime Report, Prepared by the National White Collar Crime Center and the Federal Bureau of Investigation, January 1, 2004 - December 31, 2004.

49- Al-Dharrab, Mohannad (2005) Benchmarking Framework For Software Watermarking.- King Fahd University of Petrolume and Minerals.- Available at: http://library.kfupm.edu.sa/Theses/Details.aspx?Shelflist_number=A+1.D435&Comm-Advisor-ID=40

50- El-Sheikh, Asim, Rashed, Abdullah & Peace, A. Gaham (2004), Software Piracy: Possible Causes and Cures.- Available at: http://www.drpeace.com/m493s05/Piracy.doc.

51- El-Sheikh, A., Rashed, A., Al-Qudah, B. and Peace, A. (2006) An Exploratory Study of Software Piracy in Jordan.- The Electronic Journal on Information Systems in Developing Countries, vol 23.- Available at:

https://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/188/146

52- Hinduja, Sameer. (2008) Deindividuation and Internet Software Piracy. Cyberpsychology & Behavior, Vol.11 (4).- Available at: http://online.liebertpub.com/doi/abs/10.1089/cpb.2007.0048

53- Mohamed ChaIwki ,Essai sur la notion de cybercriminalité, juillet 2006. site: www.iehei.org.